GodRAT: Gh0st-style Espionage Targeting Financial Institutions



By Mario Rojas, Senior Security Researcher, ORYXLABS

A campaign uncovered by Kaspersky in late 2024 is using malicious screen-saver (.scr) and program information (.pif) files disguised as financial documents to deploy a new remote-access trojan dubbed GodRAT.

GodRAT, an evolution of the long-standing Gh0st RAT, hides its first-stage code inside images before downloading the main payload from a C2 server. Targets include financial trading and brokerage firms in Hong Kong, the United Arab Emirates, Lebanon, Malaysia and Jordan.

The operator's tactics and ties to Winnti APT, paired with GodRAT's similarities to the AwesomePuppet backdoor, suggest that the goal is espionage rather than immediate financial theft. Organisations in the UAE should monitor key indicators (outlined below) and adopt proactive controls to mitigate the risk of attack.

Threat actor profile and strategic context

- **Motivation and attribution:** The malware's code and the unusual "puppet" command-line argument point to AwesomePuppet, a Gh0st-based tool previously linked to the Winnti APT. Winnti is known for espionage against high-value targets.

- **Target geography:** Detections have occurred in Hong Kong, the UAE, Lebanon, Malaysia and Jordan, especially in financial trading and brokerage firms.
- **Operational timeline:** The earliest artefacts date back to September 2024 and continued until at least August 2025. In the early phases, attackers relied on Skype messages to distribute weaponised .scr files; later phases involved .pif files masquerading as PDFs and ZIP archives.

Technical analysis of the attack chain

- **Steganographic loaders:** Two loader types decode shellcode, either embedded in the binary or stored in a .jpg image. Self-extracting .scr files drop legitimate-looking binaries (valve.exe) signed with an expired certificate and a loader DLL (SDL2.dll) that extracts the hidden shellcode. Persistence is achieved by creating a registry run-key pointing to the legitimate executable.
- **Second-stage delivery:** The first-stage shellcode decodes configuration data using a single-byte XOR key to obtain the C2 address and port, then requests the second stage from the server. The second stage injects the main GodRAT (ONLINE.dll) into memory and invokes its run export.
- **GodRAT capabilities:** At runtime, the malware launches itself under legitimate processes such as curl.exe or cmd.exe using a -Puppet parameter. It gathers host information (OS version, process name, user account, installed antivirus) and compresses and XOR-encodes this data before exfiltration. Supported commands include loading DLL plugins, downloading and executing files, opening URLs and modifying configuration files.
- **Plugins and implants:** The FileManager plugin performs file-system enumeration and operations such as listing, reading, writing and deleting files or launching applications. Additional payloads include password stealers for Chrome and MS Edge that harvest browser login databases and an injector for AsyncRAT that bypasses AMSI/ETW for stealth.

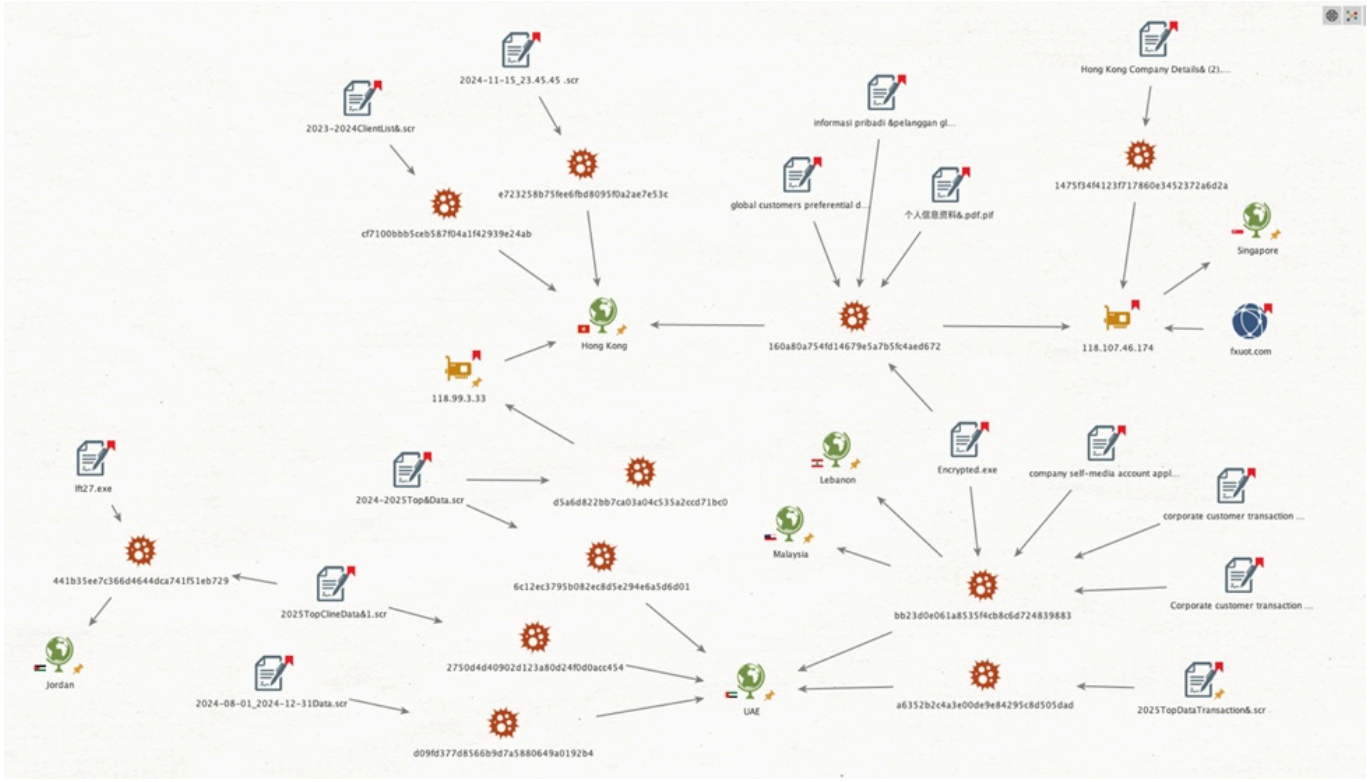
Indicators of compromise (IOCs)

The following is a non-extensive list of IOCs that were directly highlighted in Kaspersky’s original research. For the full set of indicators, please refer to the original report.

Campaign visualisation and enrichment

To better understand the relationships across the campaign, we constructed a network graph based on the IOCs. The goal was to visualise infrastructure reuse, filename patterns, and cross-regional targeting.

- The complete graph is extensive, connecting entities across several geographies.
- The screenshot below focuses on UAE-related findings.



Additional IOCs from pivoting

By pivoting off the original IOCs and shared infrastructure, we identified additional artefacts potentially connected to these campaigns. These include executables, archives, and DLLs that follow the same naming conventions (*“Data,” “Transaction,” date ranges*), suggesting continuity of social engineering lures and tool reuse.

MITRE ATT&CK mapping

Recommendations for mitigation and risk reduction

Defenders should adopt a proactive, intelligence-led approach to reduce exposure:

- **Credential breach monitoring**: Utilise digital risk monitoring solutions such as Discovery to detect compromised credentials and stolen cookies before attackers use them for lateral movement and email impersonation.
- **DNS-based threat detection**: Deploy a DNS Firewall to block connections to malicious domains and identify abnormal domain-generation patterns or steganographic C2 channels. Monitoring DNS queries can reveal attempts to reach GodRAT infrastructure.
- **Attachment and URL filtering:** Block or quarantine suspicious .scr, .pif and .zip files at email and instant-messaging gateways. Educate employees about the dangers of opening unsolicited attachments.
- **Endpoint and behaviour analytics:** Use EDR solutions capable of detecting reflective code injection, suspicious process chains (e.g., curl.exe launched by

unknown parents) and registry persistence modifications. Monitor for legitimate processes loading unknown DLLs.
- **Browser credential protection**: Encourage the use of password managers and multi-factor authentication. Regularly clear saved credentials and restrict file-system access to browser databases to hinder password stealers.

Conclusion and strategic takeaways

GodRAT demonstrates how legacy malware codebases like Gh0st RAT can be repurposed and enhanced with modern tradecraft such as steganographic loaders and modular plugins. The campaign’s focus on financial trading firms and its connection to the Winnti APT highlight the strategic value of espionage over immediate monetisation. By integrating the indicators and mitigation actions outlined above and leveraging tools such as Discovery and DNS Firewall, organisations can strengthen detection and response capabilities against this and similar threats.

There’s always more intelligence to uncover.